Cryptography Solutions

1) $6 \mid 42$, $a \mid b \Rightarrow b = ac$

$42 = 6c$, $c \in \mathbb{Z}$ so $c = 7$

b) $64 \mid 50$, $50 = 64c$, $64 \nmid 50$

c) $16 \mid 0$, $0 = 16c$, $c = 0$

d) $0 \mid 15$, $15 = 0c$, $0 \nmid 15$

2) $15 \times 29 \bmod 13$

Using the fact that

$29 \equiv 3 \bmod 13$

$15 \times 3 \bmod 13 \equiv 6 \bmod 13$

b) $2 \times 29 \bmod 13 \equiv$

$\Rightarrow 2 \times 3 \bmod 13 \equiv 6 \bmod 13$

c) $2 \times 3 \equiv 6 \mod 13$

d) $-4 \times 3 \mod 13 \equiv 9 \times 3 \mod 13$

$\equiv 1 \mod 13$

3) $[0]_7 = \{ \ldots\ldots -21, -14, -7, 0, 7, 14, \ldots \}$

$[1]_7 = \{ \ldots\ldots -13, -6, 1, 8, 15, \ldots\ldots \}$

$[2]_7 = \{ \ldots\ldots -12, -5, 2, 9, 16, \ldots \}$

$[3]_7 = \{ \ldots\ldots -11, -4, 3, 10, 17, \ldots \}$

$[4]_7 = \{ \ldots\ldots -10, -3, 4, 11, 18, \ldots \}$

$[5]_7 = \{ \ldots\ldots -9, -2, 5, 12, 19, \ldots \}$

$[6]_7 = \{ \ldots\ldots -8, -1, 6, 13, 20, \ldots \}$

4) $x \equiv 3^2 \mod 13$

$x \equiv 9 \mod 13$

b) $x \equiv 7^2 \mod 13$

$x \equiv 49 \mod 13$

$x \equiv 10 \mod 13$

c) $x \equiv 3^{10} \bmod 13$

$x \equiv (3^2)^5 \bmod 13$

$x \equiv 9^5 \bmod 13$

$x \equiv 9 \cdot 9^4 \bmod 13$

$x \equiv 9 \cdot 9^1 \cdot 9^3 \bmod 13$

$x \equiv 3 \cdot 9^3 \bmod 13$

$x \equiv 3 \cdot 9^2 \cdot 9 \bmod 13$

$x \equiv 3 \cdot 3 \cdot 9 \bmod 13$

$x \equiv 81 \bmod 13$

$x \equiv 3 \bmod 13$

d) $x \equiv 7^{100} \bmod 13$

$x \equiv (7^2)^{50} \bmod 13$

$x \equiv 10^{50} \bmod 13$

$x \equiv (10^2)^{25} \bmod 13$

$x \equiv 9^{25} \bmod 13$

$x \equiv (9^5)^5 \bmod 13$

$x \equiv 3^5 \bmod 13$

$x \equiv 9 \bmod 13$

e) Trial shows $x = 5$

$7^5 \equiv 11 \bmod 13$

$16,807$

$13 \mid 16807 - 11$ ✓

5) $a \equiv 7$ and $b = 22$

~~aa~~ $y = E_K(x) = ax + b \bmod 26$

$x = D_K(y) = a^{-1}(y - b) \bmod 26$

$a \cdot a^{-1} \equiv 1 \bmod 26$

$7 \cdot a^{-1} \equiv 1 \bmod 26$

$a^{-1} = 15$

$D_K(y) = 15(y - 22) \bmod 26$

plaintext :- First the sentence and then the evidence said the queen b)

letter	count	frequency %
A	5	0·77
B	68	10·53
C	5	0·77
D	23	3·56
E	5	0·77
F	1	0·15
G	1	0·15
H	23	3·56
I	41	6·35
J	48	7·43
K	49	7·59
L	8	1·24
M	62	9·60
N	17	2·63
O	7	1·08
P	30	4·64
Q	7	1·08
R	84	13·00
S	17	2·63
T	13	2·01
U	24	3·72
V	22	3·41
W	47	7·28
X	20	3·10
Y	19	2·94
Z	0	0

Because the practice of the basic movement of kata is the focus and mastery of self - - - -

7) WHAT FOOLS THESE MORTALS BE
PUCK PUCKP UCKPU CKPUCKP UC

Ciphertext :- LBCDU IQVHN JOHYO
YGNCV HVG

8) AVENGERS ASSEMBLE
THANOSTH ANOSTHAN

Ciphertext :- TMWAIOCP
AVWOHGPJ

9) $y = E_K(x) = (ax+b) \bmod 30$

$x = D_K(y) = a^{-1}(y-b) \bmod 30$

$a^{-1} = 23$

Plaintext :- FRODO

b) 30×8

$= 240$ keys